Advisory Alert

Alert Number : AAA20210104 **Date :** January 4, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	Medium	Multiple Vulnerabilities

Description

Affected Product	Fortinet
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities
Description	Fortinet has released security patch updates addressing multiple vulnerabilities that exists in their products. CVE-2020-15937 - This vulnerability allows a remote attacker to perform cross-site scripting (XSS) attacks and it is caused due to improper neutralization of user-supplied data in the IPS and WAF logs dashboard. CVE-2020-9295 – Due to a flaw in fortinet, FortiClient and FortiOS AV engines may not immediately detect certain types of malformed or non-standard RAR archives, potentially containing malicious files causing bypass protection.
Affected Products	FortiOS 6.2 running AV engine version 6.00142 and below. FortiOS 6.4 running AV engine version 6.00144 and below. FortiClient 6.2 running AV engine version 6.00137 and below. FortiGate version 6.2.5 and below. FortiGate version 6.4.1 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-20-068 https://www.fortiguard.com/psirt/FG-IR-20-037%20

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.